**PART I**

|  |
| --- |
| Individual Requesting and Responsible for TCP: Click here to enter text. |
| Telephone Number | Click here to enter text. |
| E-mail Address | Click here to enter text. |
| Request Date | Click here to enter a date. |
| Description of Controls (EAR/ITAR Category #) | Click here to enter text. |
| Room number(s) Covered by TCP | Click here to enter text. |
| Click here to enter text. |
|  | Name | Nationality | Export Control Training |
| Personnel who will have access to export controlled subject matter (add attachment to the end of the TCP, if applicable). ***Identify the project supervisor***. | Click here to enter text. | Click here to enter text. | Click here to enter a date. |
| Click here to enter text. | Click here to enter text. | Click here to enter a date. |
| Click here to enter text. | Click here to enter text. | Click here to enter a date. |
| Click here to enter text. | Click here to enter text. | Click here to enter a date. |
| Is sponsored research involved?  | Yes [ ]  No [ ]  |
| If yes, identify sponsor: | Click here to enter text. |
| Kuali Proposal/Award Number and projected end date of project | Click here to enter text. |
| Is a non-disclosure agreement involved?  | Yes [ ]  No [ ]  |
| If yes, identify the parties: | Click here to enter text. |
| Contact Information:  | Click here to enter text. |
| Attachments: |  Part II and III - Export Certification Form, and TCP |  |
| Approved: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_UMBC Export Controls Empowered Official | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date |

|  |
| --- |
| **PART II****CERTIFICATION ON THE HANDLING****OF EXPORT-CONTROLLED INFORMATION**  |
| The below project involves the use of Export-Controlled Information. As a result, the project implicates either the International Traffic in Arms Regulations (ITAR) under the jurisdiction of the Department of State, or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.It is unlawful under the ITAR to send or take Export-Controlled Information out of the U.S.; disclose, orally or visually, or transfer export-controlled information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, a license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students. In general, Export-Controlled Information means activities, items, and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application utility. Export-Controlled Information does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of Export-Controlled Information is military or civil in nature. Researchers may be held personally liable for violations of the ITAR and EAR. As a result, you should exercise care in using and sharing Export-Controlled Information with others. Technical information, data, materials, software, or hardware, i.e.; technology generated from this project, must be secured from use and observation by unlicensed non-U.S. citizens. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled Information up to and including incarceration. Security measures will be appropriate to the classification involved. Examples of security measures are (but not limited to):* Project Personnel – Authorized personnel must be clearly identified. Green Card holders are considered U.S. persons for purposes of export laws and are authorized to work on the project. Visitor access must be controlled.
* Campus Personnel – Access for UMBC persons from areas, such as custodial, maintenance, environmental safety and health, must be controlled and coordinated with the identified TCP supervisor or departmental chair/supervisor so that sensitive materials are securely locked away during their visit.
* Laboratory “work-in-progress” - Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
* Marking of Export-Controlled Information - Export-Controlled Information must be clearly identified and marked as export-controlled.
* Work Products - Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; preferably located in rooms with key-controlled access.
* Equipment or internal components – Such tangible items and associated operating manuals and schematic diagrams containing identified “export-controlled” technology are to be physically secured from unauthorized access.
* Electronic communications and databases – Appropriate measures will be taken to secure controlled electronic information. Such measures may include: User ID, password control, SSL or other approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology. Cloud based storage and collaboration systems, such as Google and Box, ***must*** not be used to store or share export controlled data or communications.Google stores its data around the world and employs people who are not US persons. Box data is currently stored in the US but there is no guarantee that Box will always keep and store data in the US.
* Conversations – Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

Department(s): Click here to enter text.Research Project Title: Click here to enter text.Sponsor: Click here to enter text.Certification: I hereby certify that I have read and understand this Certification, and that I understand and agree to follow the procedures outlined in the TCP. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export-Controlled Information to unauthorized persons.Signatures: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

**PART III**

**TECHNOLOGY CONTROL PLAN (TCP)**

**1) COMMITTMENT**

The University of Maryland, Baltimore County (UMBC) is committed to export controls compliance. The Office of Research Protections and Compliance is responsible for implementation of technology control plans as applicable. The Empowered Official for export controls is Dean Drake, Associate Vice President of Research. The individual who has requested this TCP in Part 1 is identified as being responsible for and committed to ensuring compliance.

**2) BACKGROUND AND DESCRIPTION OF THE USE OF CONTROLLED ITEMS AND INFORMATION**

(Summarize the scope of the export and clearly define the technical data, hardware, and/or defense services. Include background information on the full scope of the program.)

 Click here to enter text.

Estimated end date for use of controlled items and information: Click here to enter a date.

**3) PHYSICAL SECURITY AND PERSONNEL ACCESS**

Persons identified in this TCP will be screened via Visual Compliance Restricted Party Screening. Persons identified on any of the following lists, a) Denied Persons, b) Unverified, c) Entity, d) Specially Designated Nationals, and e) Debarred/Suspended will not be allowed to participate in TCP project activities. No foreign persons may begin working on the project until such authorization is obtained and activated. No additional personnel may be assigned to or have access to this project without first notifying the Empowered Official.

Summarize the following, where appropriate: Where will the work or activity be performed/conducted, how will the room be secured and who will have access to keys? Where will discussions about the project take place? How will the work areas be segregated to ensure there are no inadvertent transfers of project information or details? How will the project equipment be stored? How will visitor access be controlled?

Click here to enter text.

**NOTE: Individuals with keys or key cards are expressly prohibited from permitting others to use their keys or key cards for access to the research site. Doors to secured areas may not be propped or left open. Photographs of export-controlled items are strictly prohibited and all cell phones must remain off and stored while in the room. The Empowered Official must be contacted to approve all visitors prior to granting access to the room and will document citizenship of all visitors when making access determinations. Authorized project personnel should not share or discuss project-related information with any individual not authorized to participate in the project.**

**4) INFORMATION SECURITY**

Summarize the following, where appropriate: How will project-related laboratory notebooks and any other hard copy materials be stored? Where will electronic data be stored and who will have access to the data (***see above security***

***measure guidance***)? Will removable hard drives be used for data back-up? When not in use, where will back-up removable drives be securely locked? Who will have keys? How will access to electronic data be restricted to only those individuals authorized to access the data? How will the information/deliverable to transmit to the sponsor? Who is the assigned IT person? Is that person a U.S. person?

Click here to enter text.

**NOTE: Password protected files not stored on a network do not have to be encrypted. Any files removed from this system by any media will be encrypted. Virus protection software must be provided for these computers. If isolation is not possible, 128-bit or better encryption will be utilized to protect information. Disposal of computer floppy drives, compact discs, jump drives, portable digital media devices, and papers that contain controlled technical materials will be coordinated with the Empowered Official.**

**5) INTERNATIONAL TRAVEL**

Summarize the following, where appropriate: Will there any international travel associated with this project? If so, when and where, if known (inform the Export Controls Officer as far in advance to the trip as possible).

Click here to enter text.

**NOTE: Computers or other electronic storage devices containing restricted information should not normally be used for travel. If a computer is necessary for international travel, all unnecessary technical information not required for the trip should be removed and any information, which is required must be authorized for the destination and end use.**

**6) TRAINING AND AWARENESS**

All UMBC personnel with access to controlled information on this project have received training on the TCP via the OPRC [training page](http://research.umbc.edu/education-training/). Additional export control training for this project may be conducted by UMBC’s Office of Research Protections and Compliance. Enter date(s) when all personnel training is completed in Part 1.

**7) PROJECT TERMINATION**

Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminated when the information has been destroyed or determined to be no longer export-controlled. Please provide any additional information: Click here to enter text.

**8) COMPLIANCE ASSESSMENT**

As a critical component to the University’s ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings are reported to the Office of Research Protections and Compliance (410-455-2737 or compliance@umbc.edu). The ORPC may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the Empowered Official.